British Journal of Mathematics & Computer Science
11(4): 1-24, 2015, Article no.BJMCS.19442
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

Construction of Maximum Period Linear Feedback Shift Registers (LFSR) (Primitive Polynomials and Linear Recurring Relations)

Babacar Alassane Ndaw[1], Djiby Sow[2] and Mamadou Sanghare[2*]

[1]Central Technical Service of Cipher and Information Security Systems, Graduated of the Centre of Superior Cryptographic Studies of Paris, Department of Mathematics and Computer Science, University Cheikh Anta Diop, Dakar, Senegal.
[2]Department of Mathematics and Computer Science, University Cheikh Anta Diop, Dakar, Senegal.

Article Information

DOI: 10.9734/BJMCS/2015/19442
Editor(s):
(1) Vishnu Narayan Mishra, Department of Mathematics, Sardar Vallabhbhai National Institute of Technology, India.
Reviewers:
(1) Zhaneta Nikolova Tasheva, National Military University, Bulgaria.
(2) Octav Olteanu, University Politehnica of Bucharest, Romania.
Complete Peer review History: http://sciencedomain.org/review-history/11318

Original Research Article

Received: 10 June 2015
Accepted: 01 August 2015
Published: 08 September 2015

Abstract

Feedback Shift Register (FSR) is generally the basic element of pseudo random generators used to generate cryptographic channel or set of sequences for encryption keys. This type of generator is widely used in stream cipher and communication systems such as C.D.M.A (Code Division Multiple Access), mobile communication systems, ranging and navigating systems, spread spectrum communication systems.

The objective of the present paper is to propose a method for determining linear recurring sequences generating linear feedback shift register (LFSR) from primitive polynomials (and vice-versa). The linear recurring sequences facilitate the construction of maximum length LFSR. It also insists, in the last part, on the cryptographic security of LFSR and indicates some open problems in the area of nonlinear feedback shift registers (NLFSR) based pseudo random generators.

Keywords: Pseudo random generator; linear feedback shift register (LFSR); nonlinear feedback shift register (NLFSR); primitive feedback polynomial; linear recurrence; cryptographic security.

**Corresponding author: Email: mamadou.sanghare@ucad.edu.sn;*

1 Introduction

Contrary to blocks ciphers algorithms, stream cipher algorithms operate on every unit of the plaintext (encryption of a bit/character at time, bit by bit or character by character); the bits are encrypted individually. They are generally faster than blocks cipher algorithms, and have less complex circuits [1-18].

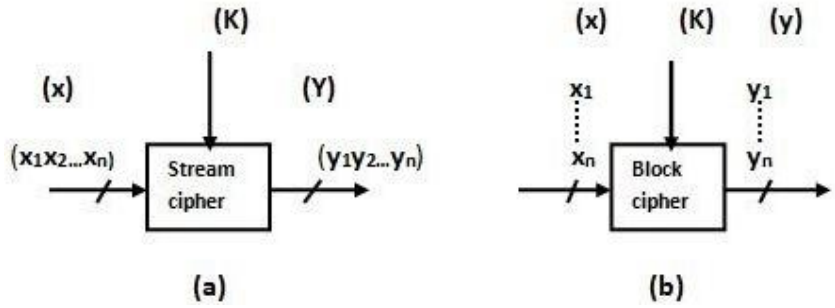


Fig. 1. (a) Stream cipher and (b) Block cipher

The stream cipher based on a key generator which generates a bit stream (Key Stream) i.e. a key sequence $K = (k_1, k_{2,.....} k_n)$ that combined (XOR function) to bits of plaintext $X = (x_1, x_2,....,x_n)$ provides ciphertext $Y = (y_{1, y2},.....,y_n)$.

- encryption equation $y_i = E_{k\,i}(x_i) = x_i \oplus k_i$
- decryption equation $x_i = D_{ki}(y_i) = y_i \oplus k_i$
  (E_{ki}=encryption function and D_{ki}=decryption function)
  Encryption is reciprocal: we encrypt as we decrypt. The key stream generator may be regarded as a finite state machine.
- An error in y_i affects only one bit x_i
- The loss or addition of a bit y_i a affects all following bits (x_i) after decryption
- if $k_i = 0$, $\forall i, X = Y$
- if the following key (k_i) is infinite and completely random, one obtain crypto system key-a-time crypto system (One-Time-Pad) also called VERNAM cipher, name of its inventor Gilbert VERNAM (1917) [2,5,6,9,10,17,19-21] which is unconditionally secure against a cipher text only attack, the cryptogram contributes no information about the plaintext.

Generally, the stream cipher is based on the same principle as the "One-Time-Pad" with the only difference that it requires a real random sequence which cannot be produced unless you know the whole sequence.

In default, pseudo-random key sequences generated by a pseudo-random generator is therefore used [12] [22-25]. Good pseudo-random sequence is one for which, knowing a portion of the sequence, it is extremely difficult, in practice, to determine the rest of the sequence [26]. A classic method for generating a pseudo random sequence [27,28] is to use a feedback shift register [cf. paragraph 2].

The bit stream (Stream Key) or sequences of keys generated by the key stream generator constitutes a cryptographic chain.

The stream cipher is classified into two (2) categories:

- Synchronous stream cipher:

  In synchronous stream cipher, the flow of bits of the key stream is generated independently both of the bits of the plaintext and the bit stream of the cipher text. The sender and receiver must be

synchronized i.e. use the key stream and be in the same condition that the decryption can be done. If there's a loss or addition of bits, the decryption fails. However, changing a bit in the transmission does not interfere in the decryption of the following bits.

Examples [2,14]: Output Feedback Mode (OFB) for block cipher systems and CTR mode (Counter Mode) are examples of synchronous stream cipher.

- Self synchronizing stream cipher or asynchronous stream cipher:

  In self-synchronizing stream cipher (or asynchronous stream cipher) each bit of the stream generated by the key generator is a function of a fixed number of bits of the preceding cryptogram. In this method, the generators are synchronized automatically.

If some encrypted bits are lost or added in the cipher text, self synchronization is always possible. However, the system is subject to error propagation, and similarly, a modification of the cipher text by the descriptor can lead in an incorrect decryption of several bits.

Example [14]: Cipher Feedback Mode (CFB) transforms block cipher into self asynchronous stream cipher.

The two (2) methods of stream cipher mentioned above are described in detail, in [1,2,6,10,12,14,19,29,30].

2 LFSR (Linear Feedback Shift Register)

An example of this type of generator is the FSR (Feedback Shift Register=Shift Registers + a feedback function).

2.1 Définition: [14,27,31-33]

- A flip- flop (position on a delay line or other memory device) is an electronic device capable of storing binary information (bits 0 and 1).
- A shift register of length (n) consists of n-flops interconnected such that the binary state of the memory cell of rank (i) is transmitted to the memory cell of rank (i + 1) when a clock signal is applied to the all flip- flops. Each flip- flop may be seen as a stage of the register. The binary information of the last stage is always accessible physically.

A shift register is then constituted of:

- An input which, in shift mode, will advance the bit of a flip- flop to a next flip- flop.
- (n) flops constituting the register stages.
- And an output.

Example of a shift-register of 11 stages:

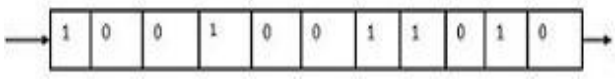


Fig. 2. 11 bits LFSR

Most pseudo-random generators are constructed using feedback shift registers (Example: eSTREAM project running from 2004 to 2008 to choose new standard stream ciphers: Sosemanuk, Grain, Mickey, Trivium) [27,31,34-39].

The Feedback Shift Registers constitute the base of pseudo-random generators used for generation of encryption key. This type of generator is largely used in stream cipher.

A Feedback Shift Register (FSR) of size (n) is an automate constructed by a boolean function (f) (ref: Definition 2.2) and a function (F) both with n variables over a field GF (p) such that F: $\{0,1\}^n \rightarrow \{0,1\}^n$ (often $p = 2$ for binary field where $p = 2^w$ for some extension field of the binary field).

$$F(x_1, x_2, \ldots, x_n) = (x_2, x_3, \ldots, x_n, f(x_1, x_2, \ldots, x_n)) \quad (1)$$

- F which is the function of the next state, gives the new state of the FSR from the prior state;
- and (f) which is the feedback function calculates the $n - th$ term of the next state;
- If $(x_1, x_2, \ldots, x_n)$ is the initial state then the application of (f) and (F) give the state sequence:

$F(x_1,x_2,\ldots,x_n) = (x_2,x_3,\ldots,x_n,x_{n+1})$; $x_{n+1} = f(x_1,x_2,\ldots,x_n)$
$F(x2,x3,\ldots,xn+1) = (x3,x4,\ldots,xn+1,xn+2)$; $xn+2 = f(x2,x3,\ldots,xn+1)$
$F(x3,x4,\ldots,xn+2) = (x4,x5,\ldots,xn,xn+1,xn+2,xn+3)$; $xn+3 = f(x3,x4,\ldots,xn+2)$
... ...

The output sequence generated by the FSR:

$$(x_i)_i \in_N = (x_1, x_2, \ldots, x_n, x_{n+1}, \ldots) \quad (2)$$

satisfies the relation of recurrence:

$$x_{i+n} = f(x_i, x_{i+1}, x_{i+2}, \ldots, x_{i+n-1}) \quad (3)$$

If the feedback function (f) is linear (ref: 2.2 Definition), the FSR is called Linear Feedback Shift.

Registers (LFSR). Otherwise, it is called Nonlinear Feedback Shift Register (NLFSR) [40].

2.2 Definition: [1,2,4,9,14,15,17,20,27,28,30-34,41-48]

• A linear feedback shift register of n bit-length (LFSR n-bits) is composed of two parts:

- One shift register containing a sequence of n bits $(x_1,\ldots,x_n)$ arranged from left to right which is the initial state of the register;
- And, a linear feedback function $f(x_1,x_2,\ldots,x_n)$

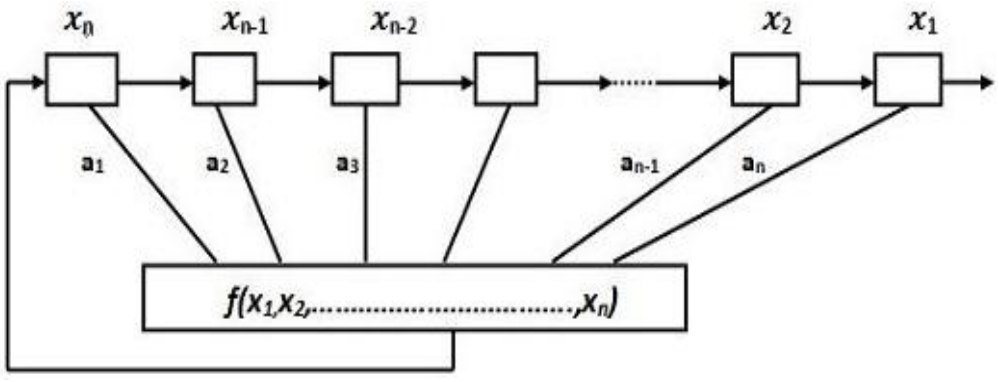


Fig. 3. General scheme of linear feedback shift register

- The registry is called by its acronym: LFSR (Linear Feedback Shift Register).
- At periodic intervals determined by the clock, the content of the stage (i) is transferred into the stage (i + 1): A bit is required at any time, and all the bits in the register are shifted forward.
- The new left most bit is obtained from the other bits in the register with the feedback function f(x_1, x_2,.....,x_n);
- Output register is 1 bit; the sequence generated is called derivation sequence (output stream)
- The period of the LFSR is the length of the sequence generated before it repeats (Ref. Definition 2.1).
- The feedback function $f(x_1,x_2,....,x_n)$ is such that:

$$f(x_1,x_2,....,x_n) = a_n x_1 + a_{n-1}x_2 + ... + a_1 x_n \quad (4)$$
$$= \sum_{i=1}^{n} a_i x_{n-i+1}$$

where $a_i = 0$ or 1 ,$\forall i$ $1 \le i \le n$, and addition (XOR operation) is over GF(2).

- $f: GF(2^n) \rightarrow GF(2)$
- f is a boolean function of (n) variables [2,30,60-64];
- There are 2^{2^n} different boolean functions for (n) variables given.
- The sequence produced by the LFSR satisfy the relation of linear recurrence:

$$a_{n+j} = \sum_{i=1}^{n} a_i x_{n+j-1} \Leftrightarrow x_{n+j} = \sum_{i=0}^{n-1} a_{i+1}\ x_{n+j-i-1} \quad (5)$$

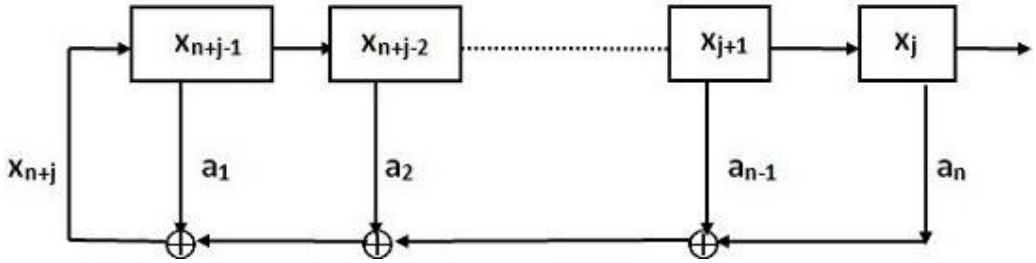


Fig. 4. A scheme of LFSR

and the matrix A associated with the linear mapping is:

$$[GF(2)]^n \rightarrow [GF(2)]^n$$
$$\begin{bmatrix} x_j \\ x_{j+1} \\ . \\ . \\ x_{n+j-2} \\ x_{n+j-1} \end{bmatrix} \rightarrow \begin{bmatrix} x_{j+1} \\ x_{j+2} \\ . \\ . \\ x_{n+j-1} \\ x_{n+j} \end{bmatrix} \quad (6)$$

$$A = \begin{pmatrix} 0 & 1 & 0 \dots . 0 & 0 \\ 0 & 0 & 1 \dots \dots 0 & 0 \\ \dots & \dots & \dots \dots \dots & \\ 0 & 0 & 0 \dots \dots 0 & 1 \\ a_n & a_{n-1} & \dots\dots\dots & a_2\ a_1 \end{pmatrix} \quad (7)$$

- Such the configuration, which we'll be interested, is called FIBONACCI's configuration (Fibonacci generator)" [2,14,28,30,45,49]. It is efficient in hardware as it requires only one n-bits LFSR and

XOR operations although inefficient in software implementation (LFSR in mode Fibonacci or External-XOR LFSR) unlike its other counterpart called GALOIS configuration (LFSR in mode Galois or internal-XOR LFSR) "discussed in [2,14,28,30].

- The Fibonacci generator or External-XOR LFSR is based on the Fibonacci's sequences modulo the maximum value desired:

$$x_n = (x_{n-1} + x_{n-2}) \pmod{m} \text{ with } x_0 \text{ and } x_1 \text{ in input} \tag{8}$$

Alternatively, we can use this form called "generalized Fibonacci" recurrences to generate pseudorandom numbers [49-51]:

$$x_n = \pm(x_{n-s} \pm x_{n-k}) \pmod{m} \text{ with } x_0 \ldots . x_{k-1} \text{ in input as words of w bits; generally } m = 2^w. \tag{9}$$

The quality of the generator depends of the coefficients (k), (s) which must be carefully chosen and the values used for the initial state of the generator. This generator is against very simple to implement and consumes little resources.

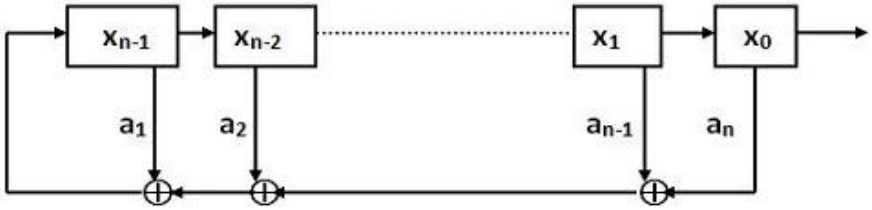


Fig. 5. LFSR in mode Fibonacci

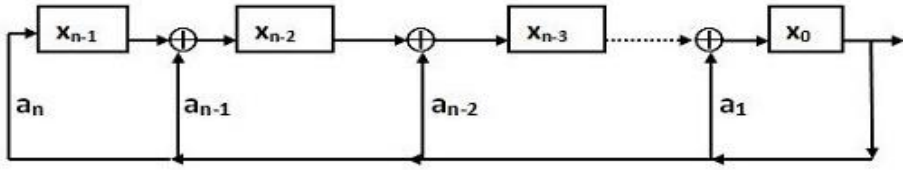


Fig. 6. LFSR in mode Galois

- We must differentiate this one from the linear congruential generator [9,14,17,30,45,52,53] that produces pseudo-random sequences of the form:

$$x_n = (ax_{n-1} + b) \pmod{m}, \text{ where } a, b \text{ and } m \text{ are integers.} \tag{10}$$

x_n is the (n)-th bit in the sequence; x_0= the seed, the period of the generator is less than m.

If a, b, and m are carefully chosen, then the generator will be said to be "maximum period (m) (e.g. If $b \wedge m = 1$,(b) and (m) are coprime), if $b = 0$, the generator is said to be homogeneous congruential multiplicative [45,52]

The linear congruential generators are fast and require little bit operations, but it has been proved that they cannot be used in cryptography for stream cipher. Indeed, they can be predicted and therefore are decryptable [14]. It is valid for:

- The Quadratic generators:

$$x_n = (ax_{n-1}^2 + bx_{n-1} + c) \pmod{m} \tag{11}$$

- The cubic generators:

$$x_n = (ax_{n-1}^3 + bx_{n-1}^2 + cx_{n-1} + d) \pmod m \quad (12)$$

discussed in [14] who notes that the combination of linear congruential generator providing long periods were not also proved safe cryptographically.

- The LFSR are used extensively in stream cipher because they are easily implemented in hardware as well as in software. Referring to the above definitions, it is possible to generalize the LFSR, in any finite $GF(p)$. On the software aspect, it is used finite field of the form $GF(2^n)$ with $n = 8, 32, 64$

2.3 Examples

Example 1: One maximal-period n-bits LFSR

A maximal-period n-bits LFSR on $GF(2)$ with maximal period $T = 2^n - 1$ is a register which can theoretically generate a pseudo-random sequence of length $T = 2^n - 1$ bits before the repetition (and not 2^n the null sequence (000...000) is not considered. The resulting output sequence is called an "m-sequence".

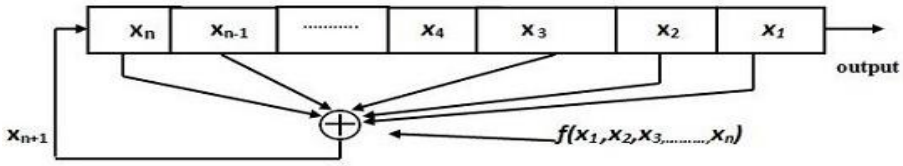


Fig. 7. n-bits LFSR

Example 2: Maximal period 3-bits LFSR. There are two possible loops:

- the stages 1 and 3: $x_{n+1} = x_n + x_{n-2} \pmod 2$ (recurrence equation)
- the stages 2 and 3: $x_{n+1} = x_{n-1} + x_{n-2} \pmod 2$ (recurrence equation)
- The loop 1 and 2 is forbidden: the LFSR loop after two steps as shown in Fig. 10 (no maximal period).

Loop 1 and 3: Maximal period. The maximal period is: $T = 2^3 - 1 = 8 - 1 = 7$.

The recurrence equation is: $x_{n+1} = x_n + x_{n-2} \pmod 2$.

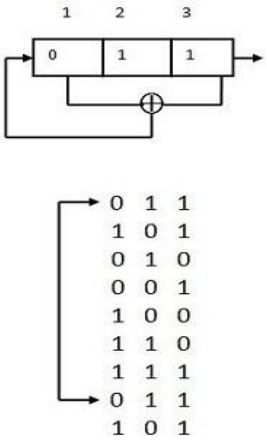
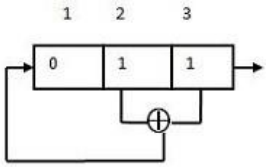


Fig. 8. 3-bits LFSR

Key stream: 1101001

Loop 2 and 3: Maximal period

The recurrence equation is: $x_{n+1} = x_{n-1} + x_{n-2} \pmod 2$



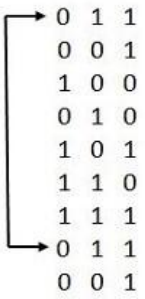
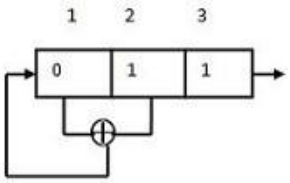


Fig. 9. 3 bits LFSR

Key stream: 1100101

Loop 1 and 2:

The recurrence equation is: $x_{n+1} = x_n + x_{n-1} \pmod 2$



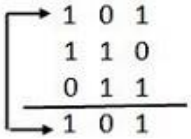


Fig. 10. 3-bits LFSR

Example 3: Maximal period 4-bits LFSR

The maximal period is $T = 2^4 - 1 = 15$ with:

Loops 1 and 4: Maximal-period

The recurrence equation is: $x_{n+1} = x_n + x_{n-3} \pmod 2$

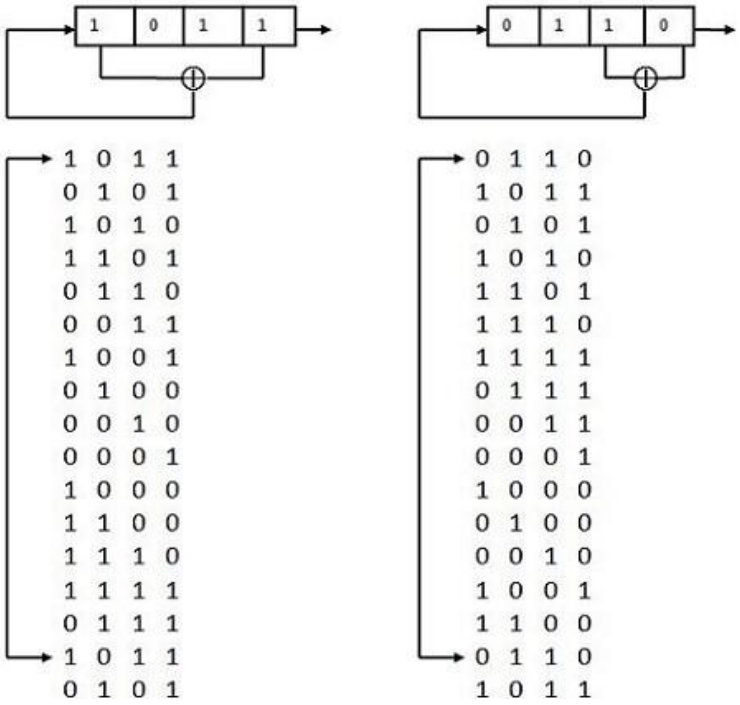


Fig. 11. 4-bits LFSR

Keys stream: 110101100100011 and 011010111100010

Loop 3 and 4: Maximal period

The recurrence equation is: $x_{n+1} = x_{n-2} + x_{n-3} \pmod 2$

Example 4: maximal period 6-bits LFSR

The maximal period is obtained by: $T = 2^6 - 1 = 63$

- the loop 1 and 6: $x_{n+1} = x_n + x_{n-5}$;
- the loop 5 and 6: $x_{n+1} = x_{n-4} + x_{n-5}$;

(Loop 5 and 6: Maximal period)

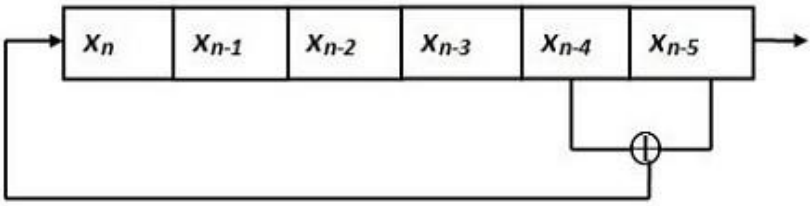


Fig. 12. 6-bits LFSR

Example 5: maximal period 31-bits LFSR

The maximal period is obtained by: $T = 2^{31} - 1 = 2.147.483.647$

- the loop 3 and 31: $x_{n+1} = x_{n-2} + x_{n-30} \pmod 2$;
- the loop 28 and 31: $x_{n+1} = x_{n-27} + x_{n-30} \pmod 2$;

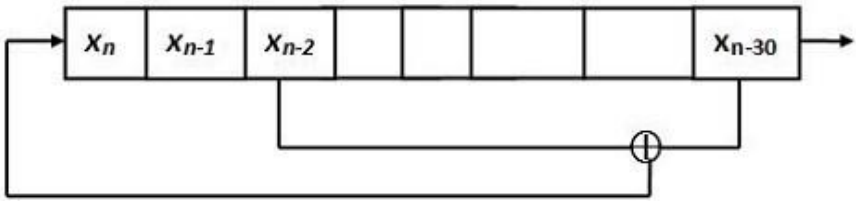


Fig. 13. 31-bits LFSR

2.4 Theorem: [4,14,28,31-34,47]

For an n-bits LFSR be maximal period, it is necessary that the polynomial formed from derivation sequence must be a primitive polynomial of degree (n) in GF (2).

- We thus associate with an n-bits LFSR, a primitive polynomial generator:

$$f(x) = 1 + \sum_{i=1}^{n} a_i x^i = 1 + a_1 x + a_2 x^2 + ... + a_n x^n \quad (13)$$

- A primitive polynomial of degree (n) is an irreducible polynomial of degree (n) which divides $(x^{2^n-1} + 1)$.

Example: the polynomial $f(x) = x^3 + x + 1$ of degree 3 is primitive over $G\,F$ (2), it divides $x^7 + 1$, ($T = 2^n - 1 = 2^3 - 1$) $\longrightarrow x^7 + 1 = (x^3 + x + 1)(x^4 + x^2 + x + 1)$.

- if any polynomial $f(x)$ associated to a LFSR is primitive over $GF(2)$ then any non-zero initial state produces a sequence of maximal period $T = 2^n - 1$.

2.5 Definition 3

Let f be a polynomial $f(x)$ in $F_2[X]$. Its order, denoted ord (f) is the smallest integer (t) such that $x^t \equiv 1 \bmod f(x)$.

2.6 Definition 4

Let $f(x)$ be an irreducible polynomial of degree (n) in $F_2[X]$. It is primitive if its order is $(2^n - 1)$.
So, we want to build an optimal n bit LFSR (in relation to the period after production), we must ensure that the feedback polynomial chosen is of degree n and primitive.

We will be sure to obtain a maximal period, but taking the precaution of using a non-zero initial state.

Another advantage of feedback primitive polynomials is the statistical quality of sequence produced.

2.7 Definition 5: [31]

Let $f(x)$ be an irreducible polynomial over $([G\,F\,(2^n)])^*$. It is called primitive if one of its roots generates the multiplicative subgroup $[GF\,(2^n)]$, with $[GF\,(2^n)] = F_2[X]/f(x)$ (polynomials reduced modulo $f(x)$). First recall that the multiplicative subgroup of a finite field is cyclic. In other words, $\forall\ \alpha \in [G\,F\,(2^n)]$, we have $\alpha^{2^n-1}= 1$.

Let (α) a root of (f), then we have $f\,(\alpha) = 0$. If α generates the multiplicative group, the elements $\alpha, \alpha^2, \alpha^3 \ldots \alpha^{2^n-1}$ correspond to all nonzero elements of the field, and there are $2^n - 1$ distinct elements ($\alpha^{2^n-1}= 1$since $\alpha \in ([G\,F\,(2^n)])^*$ cyclic).

2.8 Definition 6: [31,47]

In fact, we can define the order of an element α as the smallest (t) such that $\alpha^t = 1$. What we want to know is if the order of α is equal to $2^n - 1$ ($f(x)$ = primitive polynomial) or not ($f(x)$ = non-primitive polynomial); it must be remembered that for an n-bit LFSR, $(2^n - 1)$ and $f(x)$ divides $(x^{2^n-1} + 1)$.

Example: Let $f(x) = x^3 + x + 1$ irreducible, and (α) is as $f\,(\alpha) = 0 \Rightarrow \alpha^3 + \alpha + 1 = 0 \Rightarrow \alpha^3 = \alpha + 1$.

Let us determine the powers of α: $\alpha^1 = \alpha$

$\alpha^2 = \alpha^2$
$\alpha^3 = \alpha + 1$
$\alpha^5 = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$
$\alpha^6 = \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1$
$\alpha^7 = \alpha^3 + \alpha = 1 \Rightarrow \alpha^{2^3} - 1$ with $T = 7$.

We can conclude that the polynomial $f(x) = x^3 + x + 1$ is primitive.

3 Primitive Feedback Polynomials and Linear Recurrences for Constructing Maximal-period LFSR

With the primitive polynomial, we can identify the linear recurrence equation associated to the n−bits LFSR and vice versa.

Let the following register and the primitive polynomial defined in paragraph 2.4 (13):

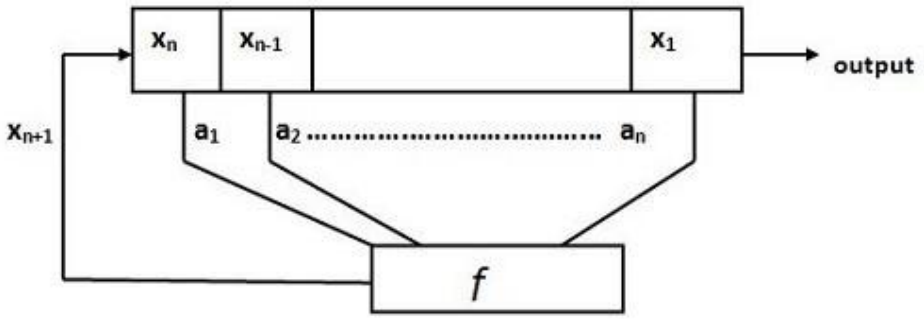


Fig. 14. n-bits LFSR

Then, our linear recurrence can be expressed in this form:

$$\begin{array}{lll} x_{n+1} & = & a_1x_n + a_2x_{n-1} + ... + a_nx_1 = \sum_{k=1}^{n-1} a_k x_{n-k+1} \\ \vdots & & \vdots \\ x_{n+i} & = a_1x_{n+i-1} + a_2x_{n+i-2} + ... + a_nx_i = \sum_{k=1}^{n} a_k x_{n-k+i} \end{array}$$

We will consider in our study, the simplest form corresponding to the single equation:

$$x_{n+1} = f(x_1, x_2, ..., x_n) = \sum_{k=1}^{n} a_k x_{n-k+1} \tag{14}$$

3.1 Maximal Period

In the case whether the polynomial generator is primitive, for all initial state of n non-zero bits, T is the maximal period: $T = 2^n - 1$.

3.2 Identification Equation

With our primitive polynomial and the linear recurrence, the identification equation is:

$$\begin{aligned} f(x) &= 1 + \sum_{k=1}^{n} a_k x^k = 1 + a_1x + a_2x^2 + ... + a_nx^n \\ x_{n+1} &= \sum_{k=1}^{n} a_k x_{n-k+1} \end{aligned} \tag{15}$$

The identification equation help us to determine the coefficients a_k and therefore the recurrence equation from the polynomial (and vice versa).

$$x_{n+1} \Leftrightarrow f(x) \tag{16}$$

3.2.1 Application to 4-bits LFSR

Let $f(x) = x^4 + x + 1$

The maximal period: $n = 4$ and $T = 2^n - 1 = 2^4 - 1 = 15$.

The identification equation:

$$\begin{aligned} f(x) &= x^4 + x + 1 \\ &= 1 + \sum_{k=1}^{4} a_k x^k \\ &= 1 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 \end{aligned} \tag{17}$$

We can identify then: $a_3 = a_2 = 0$ and $a_4 = a_1 = 1$.

But $x_{n+1} = \sum_{k=1}^{4} a_k x_{n-k+1} = a_1x_n + a_2x_{n-1} + a_3x_{n-2} + a_4x_{n-3}$, then recurrence equation is:

$x\,n+1 = a_1 xn + a_4 xn-3 \pmod 2$ (18)
$x_{n+1} = x_n + x_n-_3 \pmod 2$

we obtain the following maximal-period 4 bits LFSR:

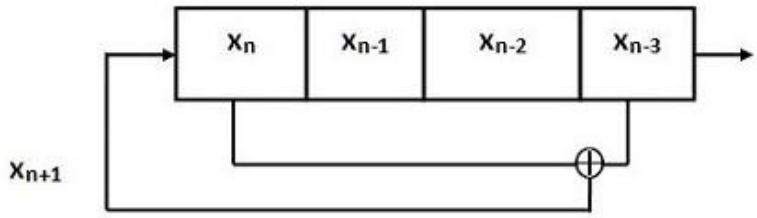


Fig. 15. 4 bits LFSR

Remark: If we make this change of variable $x = \frac{1}{x}$, we have another possible register. Indeed if $f(x)$ primitive, $g(x) = x^n f(\frac{1}{x})$ is also primitive. Assuming $f(x) = x^n + x^s + 1)$ $g(x)) = x^n f(\frac{1}{x}) = x^n(\frac{1}{x^n} + \frac{1}{x^s} + 1) = x^n + x^{n-s} + 1$ which is also primitive (reciprocal polynomial).

The two polynomials can be used to build register for applications. (More generally $f(x) = 1 + \sum_{k=1}^{n} a_k x^k$ and $g(x) = x^n + \sum_{k=1}^{n} a_k x^{n-k}$) With the polynomial $f(x) = x^4 + x + 1$, we have $g(x) = x^4 + x^3 + 1 = 1 + \sum_{k=1}^{n} a_k x^k = 1 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4$.

By using the identification equation, we have:

- $a_4 = a_3 = 1$ and $a_2 = a_1 = 0$
- $xn+1 = \sum_{k=1}^{4} a_k x_{n-k+1} = a_1 xn + a_2 xn-1 + a_3 xn-2 + a_4 xn-3$
- $\Rightarrow x\,n = xn-2 + xn-3$

We obtain then the following maximal-period 4 bits LFSR:

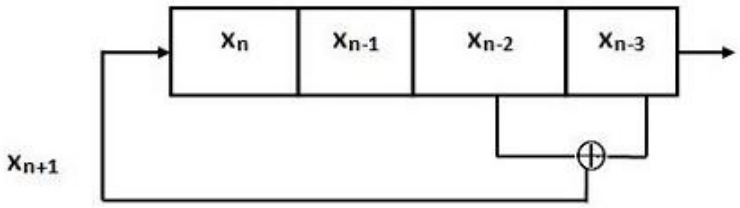


Fig. 16. 4-bits LFSR

3.2.2 Application to 35-bits LFSR

Wether: $f(x) = x^{35} + x^2 + 1$

- maximal period:
  $T = 2^n - 1 = 2^{35} - 1$
- Identification equation:

$$f(x) = x^{35} + x^2 + 1 = 1 + \sum_{k=1}^{n} a_k x_k$$
$$= 1 + a_1 x + a_2 x^2 + ... + a_{34} x^{34} + a_{35} x^{35} \quad (19)$$

All $a_k = 0$ except $a_2 = a_{35} = 1$

- $x_{n+1} = \sum_{k=1}^{35} a_k x_{n-k+1} = a_1 x_n + a_2 x_{n-1} + ... + a_{35} x_{n-34}$

• By identifying, it comes:

$$xn+1 = a_2 xn-1 + a_{35} xn-34 \quad (20)$$

$$xn+1 = xn-1 + xn-34 \quad (21)$$

We have this maximal-period 35 bits LFSR:

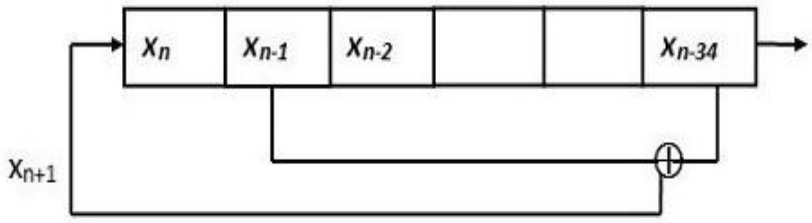


Fig. 17. 35 bits LFSR

With the usual change of variable then:

$f(x) = x^{35} + x^2 + 1 \Rightarrow g(x) = x^{35} + x^{33} + 1$ is also primitive.

$$x^{35} + x^{33} + 1 = 1 + \sum_{k=1}^{35} a_k x^k = 1 + a_1 x_+ a_2 x^2 + ... + a_{33} x^{33} + a_{34} x^{34} + a_{35} x^{35}$$

- Identification equation:

$g(x) =$

All the $a_k = 0$ except $a_{35} = 1$ and $a_{33} = 1$

$$x_{n+1} = \sum_{k=1}^{35} a_k x_{n-k+1}$$
$$= a_1 x_n + a_2 x_{n-1} + ... + a_{33} x_{n-32} + a_{34} x_{n-33} + a_{35} x_{n-34}$$
$$x_{n+1} = a_{33} x_{n-32} + a_{35} x_{n-34}$$
$$x_{n+1} = x_{n-32} + x_{n-34}$$

3.2.3 The maximal-period 35 bits LFSR

Finally, it should be noted that [45,54-56] recall some works that has been done on binary primitive polynomials and give tables of polynomials available.

However, for the realization of LFSR, it is strongly recommended to use primitive polynomials with non-zero coefficients (dense primitives polynomials) rather than polynomials among which most of the coefficients are zero and which are weak cryptographically [14].

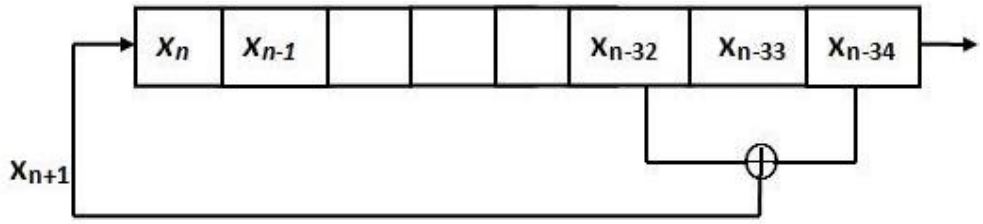


Fig. 18. 35 bits LFSR

4 Cryptographic Security

4.1 Linear Complexity

In terms of cryptographic security, the use of a single LFSR is not sure because this LFSR is predictable:

- And if we know n consecutive bits produced by an n-bits LFSR and the primitive polynomial associated, we can deduce the $(n + 1)$-th bit range produced by the register;
- If we also know $(2n)$ consecutive bits produced by an n-bits LFSR without knowing the polynomial primitive associated, we can find this polynomial by the Berlekamp-Massey algorithm [28,30,44,47,48,57,58].

This algorithm permits us to determine the linear complexity of a random sequence i.e. the length of the smallest LFSR that can generate it (also called linear span) [30,59]. In 1969, James L. Massey [44] proved, in fact, the algorithm proposed in 1967 by Ralph Elwyn Berlekamp for decoding BCH codes [57] also allows the possibility to find the smallest LFSR generating a given sequence [39] and gives a range of results on the linear complexity of random sequences.

4.2 Recommendations-Perspectives

Pseudo-random generator based on FSR used to generate keys must have the following characteristics: [12]

- A long period
- A large linear complexity
- Good statistical properties

As we noted above, the major advantage of LFSR is the ease of hardware and software implementation coupled with their good mathematical conception. However, LFSR, used alone, are not safe an account of their linearity which is exploited to build cryptanalytic attacks foremost among them the Berlekamp-Massey algorithm.

To strengthen cryptographic security of the LFSR generators, we use LFSR generators more complex using nonlinear boolean functions (cryptographic boolean function [2,30,60-64] which must have certain properties (high algebraic degree, high linear complexity, high non-linearity and high correlation immunity) that can destroy the linearity:

- Nonlinear combination generators [12,65-68]: A keystream generator on which the output of several LFSR are combined by a linear function [12,61,63]

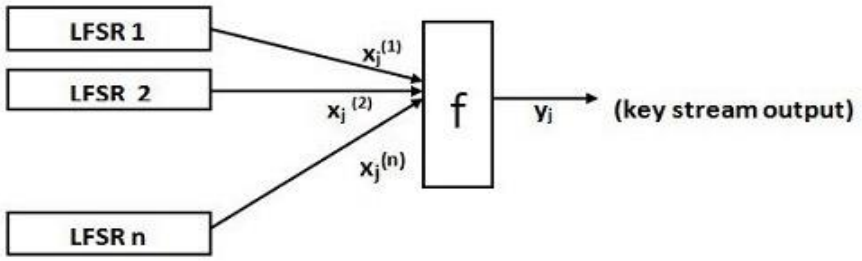


Fig. 19. Nonlinear combined LFSRs

- Nonlinear filter generator [12,69,70]: A keystream generator consisting of a single LFSR and a nonlinear function (also called Nonlinear filtering function) whose inputs are taken from some shift register stages to produce the output.

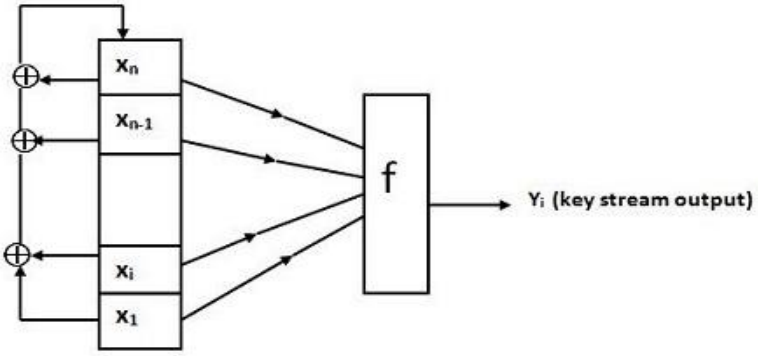


Fig. 20. Nonlinear filter generator

- Clock-controlled generator [12,71,72]: A keystream generator in which an LFSR is used to determine which output symbols of second LFSR are used as the final output.

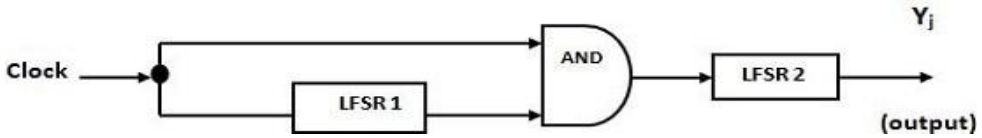


Fig. 21. Clock control

- It is also more than useful to mention the constructions concerning:

  - The shrinking generated invented in 1993, by D. Coopersmith, H. Krawczys and Y. Mansour [73] [74].
  - The self-shrinking generator invented in 1994 by W. Meier and O. Staffelback [75].

But the additional security measures have not so far allowed to shelter attacks:

- Exhaustive attacks;

- Time memory Data Tradeoff attacks [76-78];
- Correlation attacks [12,23,38,78-83]
- Algebraic attacks [38,78,80,84-88]
- Side channel attacks [38,89-91]
- Distinguishing attacks [38,92]

At present, the researches are directed to new classes of feedback Shift registers based notably on the algebraic rings, implying new methods of cryptanalysis and new security measures [28,59,93,94]. In fact, important studies have been conducted in the field of Nonlinear feedback Shift registers (NLFSR), both from the point of view of design as attacks, and which resulted:

- Since 1993 (by Andrews Klapper and Mark Goresky) to feedback with carry shift registers (FCSR) [28,93-95] in Fibonacci mode or Galois mode, with as mathematical basis, the ring of $N-$Adic integers instead of the ring of formal series used for the LFSR.

However, in spite of their large linear complexity, they are susceptible to attacks by the rational approximation algorithm [94] which is similar to that of Berlekamp-Massey.

Therefore they could be coupled with LFSR in the design of pseudo random generators.

- to vectorial feedback with carry shift registers (VFCSR), vector design of the FCSR whose analysis has been extended to finite fields $GF(p^n)$ [96].
- to Filtered feedback with carry shift registers (F-FCSR), design of FCSR to counter the attack by the rational approximation algorithm [94,97,98].
- to Algebraic feedback shift register (AFSR) when the mathematical basis is $\pi-$Adic ring (not specified as $\pi-$Adic numbers are generalizations of formal series and $N-$Adic integers). LFSR and FCSR are special cases of the AFSR [28].

It is useful to take a look also on the theory of stability of stream cipher cryptosystem i.e. the resistance of such systems to small variations in some of their parameters as regard in particular the linear complexity and nonlinear boolean functions used [3,59,99]:

- For additive synchronous stream cipher, there are already techniques of control of the stability of the linear complexity. But, the problem of the stability of the local linear complexity seems for the moment di cult to solve (this is an open problem).
- For nonlinear combined registers and nonlinear filtered register, partial results were obtained on certain aspects of the theory of stability, but research should be carried further: A promising field of research.

Other ways of research could be explored in the field of studies made, in particularly, on metric spaces and series [100,101,102].

Finally, research is also conducted on the registers with Nonlinear Update (RNLUs) which are generalization of NLFSRs whose study is theoretical and should be further refined [103,104].

5 Conclusion

As indicated at the beginning of the article, the proposed method determines mathematically, from the primitive polynomial, linear recurring relation generating the LFSR (and vice versa), and thus facilitate its construction; it also helps to establish the corresponding reciprocal primitive polynomial which gives the possibility to build another LFSR as good as the first.

We have a design and a careful choice of maximum length LFSR to use, on the basis of the primitive polynomial, the reciprocal polynomial, and associated linear recurring relations, that do not show the methods used so far where the recurrences are established, without further details, from the primitive polynomial to draw the LFSR.

On the other hand, it seemed important to review the LFSR, and to emphasize their cryptographic security with recommendations in the above paragraph and in highlighting research opportunities in this area.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Canteaut A. Stream ciphers systems. Encyclopedia of Cryptology and Security 2005, Springer Verlag; 2005.

[2] Dawson E, Simpson L. Analysis and design issues for synchronous stream cipher. Queensland University of Technology, Australia.

[3] Ding C, Xiao G, Shan W. The stability theory of stream ciphers. Department of Applied mathematics and Institute for Information security, Xidian, China, Springer Verlag; 1991.

[4] Konheim, Alan, G. Computer security and cryptography. John Wiley and Sons, Inc; 2007.

[5] Mao W. Modern cryptography. Theory and practice. Hewlett Packard Company-Prentice Hall PTR.

[6] Menezes Alfred J, Oorschot Paul CV, Vanstone A. Handbook of Applied Cryptography. CRC Press, Inc; 1997.

[7] Meyer, Carl H, Matyas, Stephen M. Cryptography: A new dimension in Computer data security, A guide for design and implementation. John Wiley and Sons Inc; 1982.

[8] Oppliger R. Contemporary cryptography. Artech House; 2005.

[9] Paar C. Applied cryptography and data security; 2005.

[10] Paar C, Pelzl J. Understanding cryptography: A Textbook for Students and Practitioners. Springer Verlag; 2010.

[11] Rothe J. Complexity theory and cryptography. Springer Verlag; 2005.

[12] Rueppel, Rainer A. Stream ciphers. Contemporary cryptology. The Science of Information Integrity, Sindia National Laboratories. IEEE Press. 1992;65-134.

[13] Schmeh K. Cryptography and public key infrastructure on internet. Wiley; 2001.

[14] Schneier B. Cryptographie appliquée, Protocoles et Codes sources en C. Thompson Publishing Vuibert; 1997.

[15] Smart N. Cryptography: An introduction. McGraw Hill.

[16] Stallings W. Cryptography and network security: Principles and practices. Prentice Hall; 2011.

[17] Trappe W. Introduction to cryptography with coding theory. Prentice Hall; 2001.

[18] Vergnaux D. Exercices et problemes de cryptographie. Dunod; 2012.

[19] QUH. Stream cipher and linear complexity. University of Maryland; 2007.

[20] Talbot J, Welsh D. Complexity and cryptography: An introduction. Cambridge University Press; 2006.

[21] Yuen PK. Practical cryptology and Web security. Pearson Education; 2006.

[22] Dumas, Jean G, Roch JL, Varrette S. Théorie des Codes. Dunod; 2007.

[23] Ebrahimi T, Leprevost F, Warusfel B. Cryptographie et sécurité des systèmes et réseaux. Lavoisier; 2007.

[24] Hersehey John E. Cryptography demystified. Mc Graw-Hill Telecom.

[25] Zemor G. Cours de cryptographie. Université de Bordeaux; 2000.

[26] Blum M, Micali S. How to generate cryptographically strong sequences of pseudorandom bits. SIAM J. Computer. 1984;13(4).

[27] Golomb, Solomon W. Shift register sequences. Aegean park Press, Laguna Hills, CA; 1982.

[28] Goresky M, Klapper A. Algebraic shift register sequences. Cambridge University Press; 2012.

[29] Foursov M. Chiffrements de flux/flot (Stream ciphers), Université de Rennes.

[30] Robshaw JB. Stream ciphers. RSA Laboratories Technical Report TR-701; 1995.

[31] Becker H, Piper F. Cipher systems, the protection of communications. Northwood Publications; 1982.

[32] Chasse G. Cryptographie mathématique. Techniques de l'Ingénieur.

[33] Mogollon M. Cryptography and security services: Mechanisms and applications. University of Dallas, USA; 2008.

[34] Details of the cryptographic principles of the MA4240-Racal Datacom limited, Milford industrial estates Tollgate Road Salisbury, Wiltshire Sp12jg (appendix 1).

[35] Babbage S, Borghoff J, Vesselin V. The estream portfolio.
Available:http://www.ecrypt.eu.org/estream/

[36] Babbage S, Canniere CD, Canteaut A, Cid C, Gilbert H, Johansson T, Parker M, Preneel B, Rijmen V, Robshaw JB. The eSTREAM portfolio.
Available:http://www.ecrypt.eu.org/estream/

[37] Mehreen A, Kansar F, Massood A. Comparative analysis of the structures of Estream submitted stream cipher. ICET 06, 245-250.

[38] Meier W. Stream ciphers, a perspective. LNCS 7374, Africacrypt 2012, Springer Verlag; 2012.

[39] Rueppel Rainer A. Analysis and design of stream ciphers. Springer Verlag; 1986.

[40] Dubrovna E. Generation of cycles by a composition of NLFSRs. Designs, Codes and Cryptography, Springer Series, Business Media. 2014;469-486.

[41] Beckett B. Cipher systems, the protection of communications. Masson; 1990.

[42] Dawson E. Linear feedback shift registers and stream ciphers.

[43] Klove T. Linear recurring sequences in boolean rings. Math. Scand. 1973;83:5- 12.

[44] Massey James L. Shift register synthesis and BCH decoding. IEEE Transaction on Information Theory. 1969;IT-15,N1.

[45] Maurin J. Simulation deterministe du hasard. Masson et Cie, Editeurs; 1975.

[46] Saluja Kewal K. Linear feedback shift register: Theory and applications. University of Winconsin. 1987;1988:1991.

[47] Song HY. Feedback shift register sequences. Yonsei University, Seoul.

[48] Van Tilborg, Henk CA. Fundamentals of cryptology. A professional reference and interactive tutorial. Kluwee Academic Publishers; 2000.

[49] Anderson R. On fibonacci keystream generators. Lecture notes in Computer science, Fast Software Encryption. 1994;1008:346-352.

[50] Brent Richard P. On the periods of generalized fibonacci recurrences. Lecture Notes in Computer Science, Fast software encryption, 12th International Conference Workshop FSE. 1992;3557.

[51] L'ecuyer P. Uniform random number generator, Annals of operations research.

[52] Downham DY, Roberts FDK. Multiplicative congruential pseudo-random generators. Department of Computational and Statistical Science, The University, Liverpool.

[53] Kurita Y. Une méthode pour choisir les paramètres d'un générateur de nombres aléatoires congruentiels. Laboratoire National de Recherches en Météorologie. 1996;104-113.

[54] Hansen T, Mullen Gary L. Primitive polynomials over finite fields. Mathematics of Computation. 1992;59(200):639-643.

[55] Zierler N. Primitive trinomials whose degree is a mersenne exponent. Information and Control. 1969;15:67-69.

[56] Zivkovic M. A table of primitive binary polynomials. Mathematics of Computation. 1994;69.

[57] Berlekamp Elwyn R. Algebraic coding theory. Mc Graw-Hill; 1967.

[58] Stamp M, Low Richard M. Applied cryptanalysis, breaking cipher in the real world. John Wiley and Sons; 2007.

[59] Cusick TW, Ding C, Renvall A. Stream ciphers and number theory. North-Hollow Mathematical Library, Elsevier Sciences BV; 1998.

[60] Braeken A. Cryptographic properties of boolean functions and S-boxes. PhD thesis, Department Electrical Engineering ESTA/COSIC, Universiteit Leuven, Belgium; 2006.

[61] Braeken A, Semaev I. The ANF of the composition of addition and multiplication mod2n with a boolean function. LNCS, Fast software encryption, 12th International Conference Workshop FSE. 2005;3557:121-134.

[62] Deepak Kumar D, Gupta Kishan C, Maitra S. Cryptographically significant boolean functions: Construction and analysis in terms of algebraic immunity. Lecture Notes in Computer Science, Fast Software Encryption, 12th International Conference Workshop, Paris. 2005;3557:107-120.

[63] Gupta Kishan C. Cryptographic and combinatorial properties of boolean functions and S-Boxes. PhD thesis, Applied Statistics Unit, Indian Statistical Institute; 2004.

[64] Preneel B, Logachev Oleg A. Boolean functions in cryptology and information security. Proceedings of the NATO. Advanced Study Institute on Boolean Functions, IOS Press. 2007;18.

[65] Canteaut A. Combination generator. Encyclopedia of Cryptology and Security 2011, Springer Verlag. 2011;222-224.

[66] Geffe PR. How to protect data with ciphers are really hard to break. Electronics. 1973;99-101.

[67] Golic Jovan D. Cryptanalysis of alledged A5 stream cipher. Advances in Cryptology, Eurocrypt. 2011;97(1233):239-255.

[68] Wei S. On generalization of Geffe's generator. International Journal of Computer Science and Network Security. 2006;6n8A.

[69] Canteaut A. Filter generator. Encyclopedia of Cryptology and Security, Springer Verlag. 2011;458-460.

[70] Golic Jovan D. On the security of nonlinear filter generator. Fast software encryption, LNCS, Springer Verlag. 1996;1039:173-188.

[71] Beth T, Piper F. The stop-and-go generator. LNCS 209; Advances in Cryptology-Eurocrypt. Springer Verlag. 1985;84:88-92.

[72] Chambers WG, Gollman D. Clock-controlled shift registers. IEEE Journal on Selected Areas in Communications. 1989;7(4):525-533.

[73] Blöcher U, Dichtl M. Fish: A fast software stream cipher, in fast software encryption. Lecture Notes in Computer Science. Springer. 2000;809:56-63.

[74] Coppersmith D, Krawczys H, Yishay M. The shrinking generator. Lecture notes in computer science. Advances in Cryptology, Crypto, Springer Verlag. 1994;773(93):22-39.

[75] Meier W, Staffelback O. The self-shrinking generator. Lecture notes in computer science. Advances in Cryptology, Eurocrypt, Springer Verlag. 1994;94:205 -214.

[76] Babbage S. Space time-off in exhaustive search attacks on stream ciphers. European. Convention on Security and Detection, IEEE Conference Publication. 1995;408.

[77] Birynkov B, Shamir A. Cryptanalytic time memory data trade-off for stream cipher. Lecture notes in computer science. Asiacrypt, Springer Verlag. 2000;976:1-13.

[78] Joux A. Cryptography and network security, algorithmic cryptanalysis. CRC Press Taylor and Francis Group; 2009.

[79] Golic Jovan D, Salmasizadeh M, Simpson L, Dawson E. Fast correlation attacks on nonlinear filter generator. Information Processing Letters. 1997;64(1):37-42.

[80] Joux A, Berbain C, Gilbert H. Algebraic correlation attacks against linearly filtered nonlinear feedback shift registers. Lecture Notes in Computer Science. Springer Verlag. 2009;5381:184-198.

[81] Meier W, Staffelback O. Fast correlation attacks on certain stream ciphers. Journal of Cryptology. 1992;3:67- 86.

[82] Salmasizadeh M, Simpson L, Golic Jovan D, Dawson E. Fast correlation attacks and multiple linear approximation. Information Security and Privacy, LNCS, Springer Verlag. 1997;1270:228-239.

[83] Stengenthaler T. Decrypting a class of stream cipher using ciphertext only. IEEE Transactions on Computers. 1985;C-34:81-85.

[84] Courtois Nicolas T. Fast algebraic attacks on stream cipher with linear feedback. Lecture Notes in Computer Science, CRYPTO, Springer Verlag. 2003; 2729:176-194.

[85] Courtois Nicolas T, Meier W. Algebraic attacks on stream ciphers with linear feedback. Lecture notes in computer science. Eurocrypt. Springer Verlag. 2003;2656:345-350.

[86] Debraize B, Goubin L. Guess-and-determine algebraic attacks on the self-shrinking generation. Lecture notes in computer science. Fast Software Encryption. Springer Verlag. 2008;5086:235- 252.

[87] Lee Dong H. Algebraic attacks on stream ciphers (a survey). Trends in Mathematics. Information Center for Mathematical Science. 2005;8:133-143.

[88] Limniotis K. Algebraic attacks on stream ciphers-recent development and new results. Journal of Applied Mathematics and Bio Informatics. Scienpress Ltd. 2013;3(1):57-5-81.

[89] Joux A, Delauney P. Galois LFSR embedded devices and side channel attacks weaknesses. Progress in Cryptology-INDOCRYPT 2006, LNCS 4329, Springer Verlag. 2006;436-451.

[90] Kocher Paul C. Timing attacks on implementation of Diffe- Hellman, RSA, DSS and other systems. Crypto 96, LNCS 1109, Springer Verlag. 1996;104-113.

[91] Strobel D. Side channel analysis attacks on stream ciphers. PhD thesis, Universitat Bochum; 2009.

[92] Hell M, Johansson T, Brynielson L. An overview of distinguishing attacks on stream ciphers. Cryptography and Communication. Springer Verlag. 2008;1(1):71-94.

[93] Klapper A, Goresky M. 2-adic shift register. Fast software Encryption, LNCS 809, 174-178.

[94] Klapper A, Goresky M. Feedback shift registers, 2-adic span and combiners with memory. Journal of Cryptology. 1997;10:2.

[95] Klapper A. A survey of feedback with carry shift register. SETA, LNCS 3486, Springer Verlag. 2005; 56-71.

[96] Allailou B. Conception et evaluation des générateurs d'Alea. PhD thesis, Université de Paris 8 (Laboratoire d'Analyse, de Géométrie et Applications-LAGA); 2010.

[97] Arnault F, Berger TP. F-FCSR, design of new class of stream cipher. Lecture Notes in Computer Science, Fast Software Encryption. 2005;3557:83-97.

[98] Arnault F, Berger TP, Lauradoux C. F-FCSR stream cipher. Lecture Notes in Computer Science, New Stream Cipher Designs, The eSTREAM Finalists. 2005;4986:170-178.

[99] Ding C. The stability theory of stream ciphers. Department of Computer Science and Engineering, The Hong Kong University of Science and Technology; 2011.

[100] Mishra VN. Some problems on approximations of functions in banach spaces. PhD thesis, Indian Institute of Technology, Roorkee- 247 667, Uttarakhand, India; 2007.

[101] Mishra VN, Mishra LN. Trigonometric approximation of signals (functions) in Lp ($p \geq 1$) norm. International Journal of Contemporary Mathematical Sciences. 2012;7(19):909-918.

[102] Deepmala. A study on fixed point theorems for nonlinear contractions and its applications. PhD thesis, Pt. Ravishankar Shukla University, Raipur (Chhatisgarh) India 492 010; 2014.

[103] Dubrovna E, Li N. An algorithm for constructing a smallest register with nonlinear update generating a given sequence. Proceeding of IEEE International Symposium on Multiple-valued Logic (ISMVL 2014). 2014;254-259.

[104] Rijmen V. Stream cipher and the estream project. The ISC International Journal of Information Security. 2010;3-11.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://sciencedomain.org/review-history/11318